Круговой многочлен

Определение: Комплексное число z называется ***примитивным корнем*** степени n из 1, если $z^n = 1$, но $z^k \neq 1$ при $1 \leqslant k < n$.

1 Докажите, что

(a) Любой корень степени n из 1 является степенью примитивного корня;

(b) Число $\varepsilon_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ — примитивный корень степени n из 1;

(c) Все примитивные корни степени n из 1 имеют вид $\varepsilon_d = \cos\frac{2\pi d}{n} + i\sin\frac{2\pi d}{n}$, где НОД$(d, n) = 1$;

(d) Если ε — примитивный корень степени n из 1, то все примитивные корни степени n из 1 имеют вид ε^d, где НОД$(d, n) = 1$

Определение: *Круговой многочлен* (или многочлен деления круга, или циклотомический многочлен) — это многочлен $\Phi_n(x) = \prod(x - \varepsilon_k)$, где ε_k — все примитивные корни степени n из 1. Ясно, что $\Phi_n(x) = \prod\limits_{d,(d,n)=1}(x - \varepsilon^d)$, где ε — любой примитивный корень степени n из 1.

2 (a) Найдите явно $\Phi_n(x)$ для $n = 2, 3, 5$.

(b) Чему равна степень $\Phi_n(x)$?

(c) Докажите, что $x^n - 1 = \prod\limits_{d|n}\Phi_d(x)$.

(d) Найдите явно $\Phi_{81}(x)$; $\Phi_n(x)$, если $n = p^k$, p — простое.

(e) Докажите, что $\Phi_n(x) \in \mathbb{Z}[x]$.

Замечание. Во всех примерах коэффициенты $\Phi_n(x)$ принадлежат множеству $\{-1, 0, 1\}$. Однако это не всегда так! Наименьшее n, при котором это не так — $n = 105$. Вообще, любое целое число встречается среди коэффициентов.

3 Пусть p — простое число. Докажите, что:

(a) Если $p|n$, то $\Phi_n(x^p) = \Phi_{np}(x)$;

(b) Если p не делит n, то $\Phi_n(x^p) = \Phi_{np}(x)\Phi_n(x)$;

(c) Если n — нечётно, то $\Phi_n(-x) = \Phi_{2n}(x)$;

Подсказка: воспользоваться задачей 2(b).

4 Докажите, что если $(n, a) = 1$, то $\Phi_n(x^a) = \prod\limits_{d|a}\Phi_{nd}(x)$.

5 Даны натуральные $n, k > 1$. Докажите, что $\Phi_n(k) \geq 2$.

6 Докажите, что в следующей бесконечной последовательности нет простых чисел:

$$10001, 100010001, 1000100010001, \ldots$$

7 Докажите, что число $2^{2^n} + 2^{2^{n-1}} + 1$ раскладывается в произведение по крайней мере n простых чисел (не обязательно различных).

8 Докажите, что $\Phi_n(x)$ — возвратный многочлен. (Многочлен $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ называется возвратным, если $a_k = a_{n-k}, 0 \le k \le n$.)

9 Найдите $\Phi_n(1)$.

10 Докажите, что для каждого многочлена $f(x) \in \mathbb{Z}[x]$ найдётся такой ненулевой многочлен $g(x) \in \mathbb{Z}[x]$, что $g(x^{10})$ делится на $f(x)$.

Теорема 1. Если $\Phi_n(a) \vdots p$, то:

- или показатель a по модулю p равен в точности n (в частности, $p - 1 \vdots n$);
- или $n \vdots p$.

11 Что означает эта теорема при $n = 4$?

12 Верно ли, что если выполнен один из пунктов заключения теоремы, то $\Phi_n(a) \vdots p$?

13 Докажите, что все простые делители числа $m^2 + m + 1$ или равны 3, или имеют вид $6k + 1$.

14 Докажите частный случай теоремы Дирихле: для любого натурального n существует бесконечно много простых чисел вида $nk + 1$.

Докажем теорему 1.

15 Рассмотрим сначала случай $p = 2$. Чему равно (a) $\Phi_n(0)$? (b) $\Phi_n(1)$? (c) Докажите, что $\Phi_n(a)$ чётно только при $n = 2^k$.

16 (a) Докажите, что $x^n - 1 = \Phi_n(x)Q(x)$, где $Q(x) \vdots x^d - 1$ для всех $d|n$, $d < n$.

(b) Пусть в условии теоремы 1 показатель a по модулю p равен $d < n$. Докажите, что тогда $\frac{n}{d} \vdots p$. Завершите доказательство теоремы 1.

Теорема 2. Если $\Phi_n(a) \vdots p$, $\Phi_m(a) \vdots p$, то $\frac{m}{n} = p^l$. В частности, при $m \neq n$ верно, что $(\Phi_n(a), \Phi_m(a)) = p^s$.

17 **Докажем теорему 2.**

(a) Докажите её для $p = 2$.

(b) Докажите усиление **16(b)** при $p \neq 2$: пусть показатель a по модулю p равен d и $\Phi_n(a) \vdots p$. Тогда $\frac{n}{d} = p^k$.

Завершите доказательство теоремы 2.

18 Докажите, что при $a > 1$ число $a^{10} + a^5 + 1$ не является степенью простого числа.

19 Докажите, что число $2^{2^n} + 2^{2^{n-1}} + 1$ раскладывается в произведение по крайней мере n *различных* простых чисел.

20 Даны попарно различные простые числа $p_1, p_2, \ldots, p_n$. Докажите, что число $2^{p_1 p_2 \cdots p_n} + 1$ имеет хотя бы $2^{2^{n-1}}$ делителей.